

МЕТОДИ МОНИТОРИНГУ ТА АНАЛІЗУ ТРАФІКУ КОМП'ЮТЕРНОЇ МЕРЕЖІ

Завдання аналізу мережевого трафіку набуває все більшої актуальності в зв'язку з розвитком і впровадженням нових мережевих технологій, а також появою великої кількості нових мережевих протоколів.

Аналіз мережевого трафіку дозволяє досягти наступних цілей:

1. Виявити в мережі шкідливе і несанкціоноване програмне забезпечення.
2. Перехопити будь-який незашифрований користувацький трафік з метою його аналізу.
3. Локалізувати несправність мережі або помилку конфігурації мережевих сервісів.
4. Виявити паразитуючий, вірусний і кільцевий трафік, наявність якого збільшує завантаження мережевого обладнання та каналів зв'язку.

Мережевий трафік є одним з найважливіших фактичних показників роботи комп'ютерної мережі і є носієм інформації про поведінку користувачів. Аналіз мережевого трафіку може бути здійснений на декількох абстрактних рівнях: на рівні номерів портів, вмісту пакету, потоку, заголовку пакету, на рівні біту.

Аналіз трафіку комп'ютерної мережі здійснюється для того щоб отримати поглиблене уявлення про те, який тип трафіку/мережевих пакетів або даних проходить через мережу.

Література

1. Маркин Ю.В., Санаров А.С. Обзор современных инструментов анализа сетевого трафика : автореф. дис. на получение наук. степени докт. / Маркин Ю.В., Санаров А.С. – г Москва. – 24 с.
2. Рошан П., Лиэри Дж. Основы построения беспроводных локальных сетей стандарта 802.11 // – М. : Издательский дом «Вильямс», 2004. – 304 с
3. Енюков И.С. Статистический анализ и мониторинг научнообразовательных интернет-сетей [Текст] / И.С. Енюков, И.В. Ретинская; под. ред. А.Н. Тихонова. – М. : Финансы и статистика, 2004. – 320 с.
4. Муранов О.С. Експериментальні дослідження механізмів прогнозування пульсацій пакетного трафіку / О.С. Муранов // Защита информации : сб. науч. трудов Национального авиационного университета. – К. : Изд-во НАУ, 2008. – Специальный выпуск. – С. 137 – 142.